เฉียงทัน เทคนิคไวรัสคอมพิวเตอร์

"บทความนี้มิได้มีเจตนาที่จะส่งเสริมให้มีการสร้างไวรัส แต่เขียนขึ้นเพื่อให้เข้าใจเทคนิคต่าง ๆ ที่จะใช้ในการสร้างไวรัส เพื่อว่าจะใช้เป็นความรู้ความเข้าใจในการป้องกันและปราบปรามไวรัสในโอกาสต่อไป"

ยืน ภู่วรวรรณ

ไวรัส มหาภัยมนุษย์โลก

หากย้อนรอยไปในประวัติศาสตร์ พบว่าไวรัสเป็นตัวสร้างปัญหาให้กับโลกมาแล้วหลายยุคหลายสมัย จากหลักฐานทางประวัติศาสตร์พบว่าไข้ทรพิษหรือฝีดาษซึ่งเป็นไวรัสตัวหนึ่งได้ผลาญชีวิตมนุษย์โลกไปไม่ใช่น้อย มนุษย์มีความพยายามคิดค้นวัคซีนเพื่อป้องกัน ในที่สุดก็มีการปลูกฝีกันอย่างแพร่หลาย มนุษย์สามารถเอาชนะไวรัสตัวนี้ได้อย่างราบคาบ จนเด็ก ๆ ในปัจจุบันไม่รู้จักกับการปลูกฝีอีกแล้ว

ไวรัสก็มีพันธุ์ใหม่เกิดขึ้นท้าทายตลอดเวลาเช่น ไวรัสของตับอักเสบชนิดบี และเราก็สามารถรู้จักกับมันอย่างดี จนสามารถแยกแยะยีนของไวรัส ตัดต่อมันมาสร้างวัคซีนจนได้ และมหาภัยไวรัสตัวที่น่ากลัวที่สุดก็อุบัติขึ้นใหม่ คราวนี้ไวรัสตัวนี้มีการปรับตัวเองตลอดเวลาจนยากที่มนุษย์จะสร้างวัคซีนได้ และเมื่อใครเอ่ยถึงไวรัสตัวนี้ทุกคนก็ได้แต่สยองไวรัสตัวนี้ คือ "เอดส์" โรคที่เป็นแล้วไม่มีทางรักษาได้ในปัจจุบัน

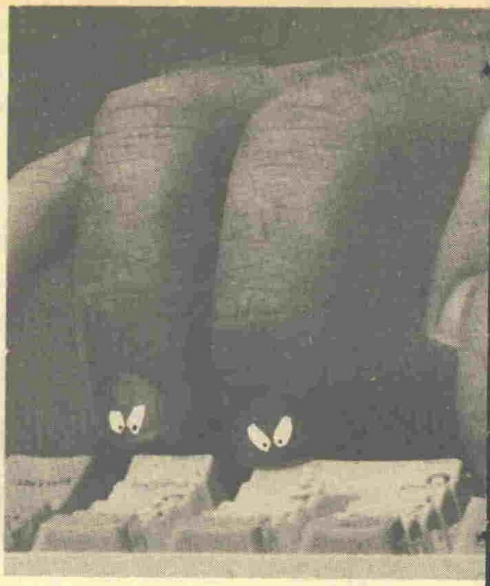
สภาพโครงร่างของไวรัสที่เกิดขึ้นกับซอฟต์แวร์คอมพิวเตอร์ก็เหมือนกับไวรัสที่ทำให้เกิดโรค แต่ไวรัสนี้เป็นไวรัสที่มนุษย์สร้างขึ้นมา อาจจะด้วยเหตุผลของความสนุกคึกคะนอง หรือลองของก็ตาม หรืออาจจะด้วยเหตุผลของคนสร้างที่ไม่เป็นปกติก็ตาม ไวรัสก็ได้แพร่กระจายออกมาก็สร้างปัญหาให้กับชาวคอมพิวเตอร์มาแล้วไม่ใช่น้อย

ไวรัสคอมพิวเตอร์คืออะไรกันแน่

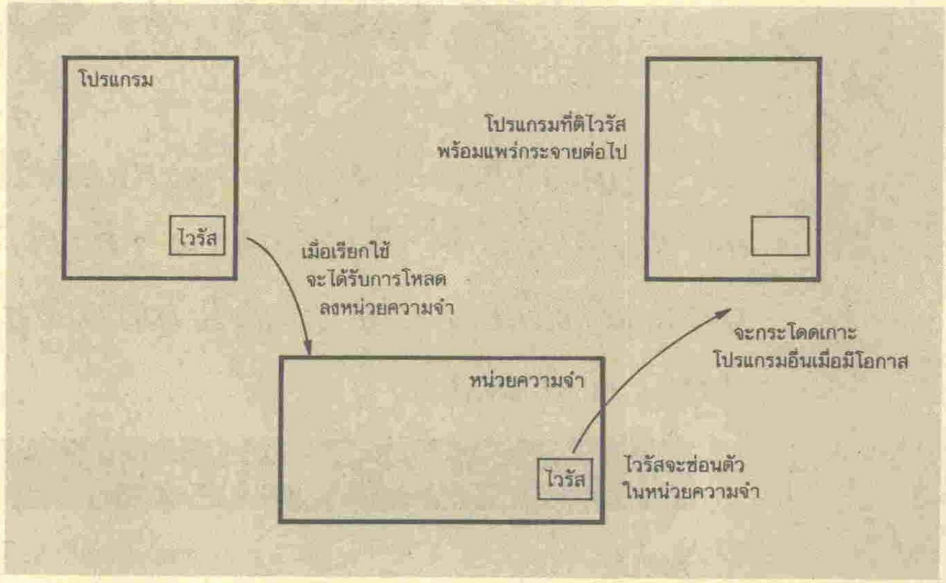
หากจะหาคำนิยามไวรัสคอมพิวเตอร์ในปัจจุบันก็คงยังไม่มีใครนิยามไว้โดยตรง ดิกชันนารีคอมพิวเตอร์ก็ยังไม่บัญญัติศัพท์คำนี้ไว้ แต่จากพฤติการของไวรัสคอมพิวเตอร์ มันคือโปรแกรมคอมพิวเตอร์โปรแกรมหนึ่งที่มนุษย์สร้างขึ้นมา โดยตัวมันเองจะแอบเกาะติดกับโปรแกรม และแพร่กระจายเกาะไปยังโปรแกรมอื่น ๆ อีกได้ อัตราการแพร่กระจายก็มีหลายรูปแบบ ขึ้นอยู่กับวิธีการที่มนุษย์ผู้ออกแบบโปรแกรม อัตราการทำลายก็ขึ้นอยู่กับผู้ออกแบบไวรัสที่จะให้ความปราณีเพียงไร

ไวรัสจึงเป็นโปรแกรมคอมพิวเตอร์ที่สามารถคัดลอกตัวเองให้ไปอยู่ยังที่อื่น ๆ โดยเฉพาะแพร่กระจายออกไป และอาจจะมีการทำลายข้อมูลหรือโปรแกรมอื่นตามเงื่อนไขของผู้เขียนโปรแกรมไวรัสได้วางไว้ บางทีจึงเรียกโปรแกรมลักษณะนี้ว่า ตัวหนอน (“worm”) ซึ่งก็หมายถึง มันไชเข้าไปในส่วนต่าง ๆ ของโปรแกรมหรือข้อมูลทำให้บางส่วนของข้อมูลหรือโปรแกรมนั้นเสียหายไปได้ แต่การที่เรียกว่าไวรัสก็เพราะว่ามันสามารถแพร่กระจายจากที่หนึ่งไปยังอีกที่หนึ่ง หรือแพร่ขยายได้อย่างรวดเร็ว อัตราการติดเชื้อนี้ขึ้นอยู่กับสภาพสิ่งแวดล้อมของตัวไวรัส อย่างไรก็ตามด้านเทคโนโลยีขณะนี้ยังไม่มีไวรัสตัวใดที่แพร่ทับโปรแกรมจัดระบบงานได้ ไวรัสแต่ละตัวจะแพร่ขยายไปบนโปรแกรมของเครื่องที่ใช้โอเอสเดียวกันเท่านั้น แต่อย่างไรก็ตามก็มีผู้พยายามสร้างไวรัสในโอเอสต่าง ๆ กันมากขึ้น จนในปัจจุบันมีการพบไวรัสในโอเอสต่าง ๆ หลายตัวด้วยกัน ทั้งบนไมโคร มินิหรือเมนเฟรม

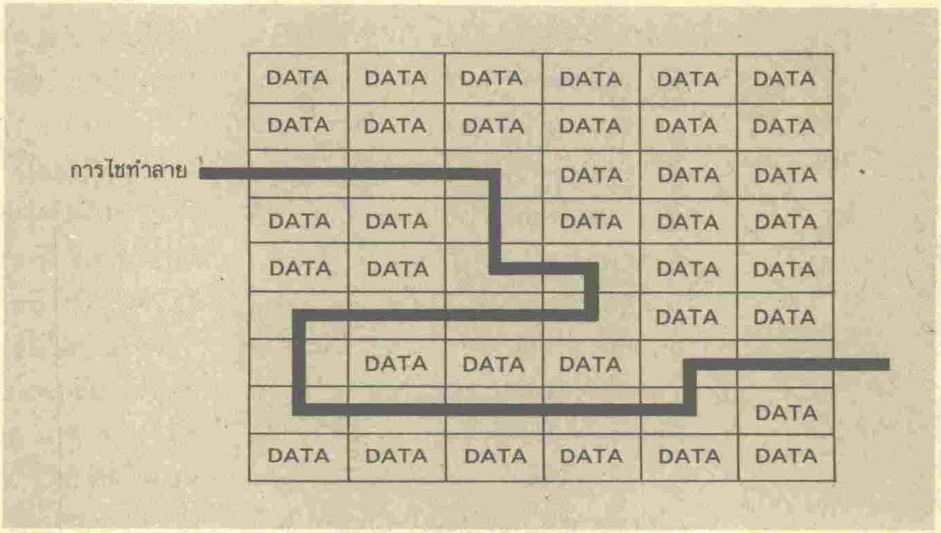
ไวรัสจะแพร่ผ่านทางใดได้บ้าง



ผู้เขียนไวรัสรุ่นใหม่มีความรู้ทางเทคนิคสูงขึ้นพอควร จึงพยายามสร้างไวรัสให้สามารถแพร่กระจายได้มากที่สุดเท่าที่จะมากได้ เช่น ให้ตัวไวรัสเกาะโปรแกรมในระดับออปเจ็คโค้ดไว้ ถ้าโปรแกรมนี้แพร่ไปทางใด ไปอยู่ที่ใด



รูปที่ 1 โครงสร้างการแพร่กระจายของตัวไวรัส



รูปที่ 2 ข้อมูลเซกเตอร์ต่าง ๆ ในดิสค์ที่ถูกไชทำลาย

ก็จะแพร่ติดโปรแกรมอื่น ๆ บนเครื่องทั้งหมด ดังนั้นการถ่ายเทโปรแกรมร่วมกันก็จะมีโอกาสแพร่กระจายไวรัสไปได้อย่างรวดเร็ว และจะติดเข้าทุกโปรแกรมที่มันอยู่ร่วมด้วย หนทางที่จะติดต่อได้จึงมีมากมายดังตัวอย่างในรูปที่ 3

รูปที่ 3
โครงสร้างการแพร่ขยายของไวรัส

ไวรัสจะทำอะไรกับระบบได้บ้าง

เคยมีบทความเสนอในเรื่องเกี่ยวกับประสบการณ์ผู้พบไวรัสในที่ต่าง ๆ ซึ่งเป็นเรื่องที่ตื่นเต้น บางเรื่องเหมือนเป็นเรื่องในภาพยนตร์วิทยาศาสตร์ บางเรื่องก็เป็นเรื่องที่สร้างความเสียหายอย่างมาก เช่น จากรายงานผู้ใช้ในการใช้งานเมนเฟรมบอกว่า ขณะใช้อยู่ปรากฏการณ์ก็เกิดขึ้นโดยมีภาพอันไม่พึงประสงค์อย่างยิ่งปรากฏบนจอภาพ สักครู่ก็มีข้อความปรากฏว่า "เราจัดการเรียบร้อยแล้ว" เป็นอันว่าข้อมูลและโปรแกรมในคอมพิวเตอร์ได้รับการทำลายไปเป็นจำนวนมาก

จากโครงสร้างของระบบคอมพิวเตอร์ในปัจจุบันที่เป็นระบบไมโครคอมพิวเตอร์ ปรากฏว่ามีการแลกเปลี่ยนข้อมูลข่าวสารกันมาก ผู้ใช้คนหนึ่งอาจต้องคัดลอกโปรแกรมหรือข้อมูลของผู้อื่นอยู่เสมอ ดังนั้นจึงมีโอกาสติดไวรัสได้ทุกเมื่อ

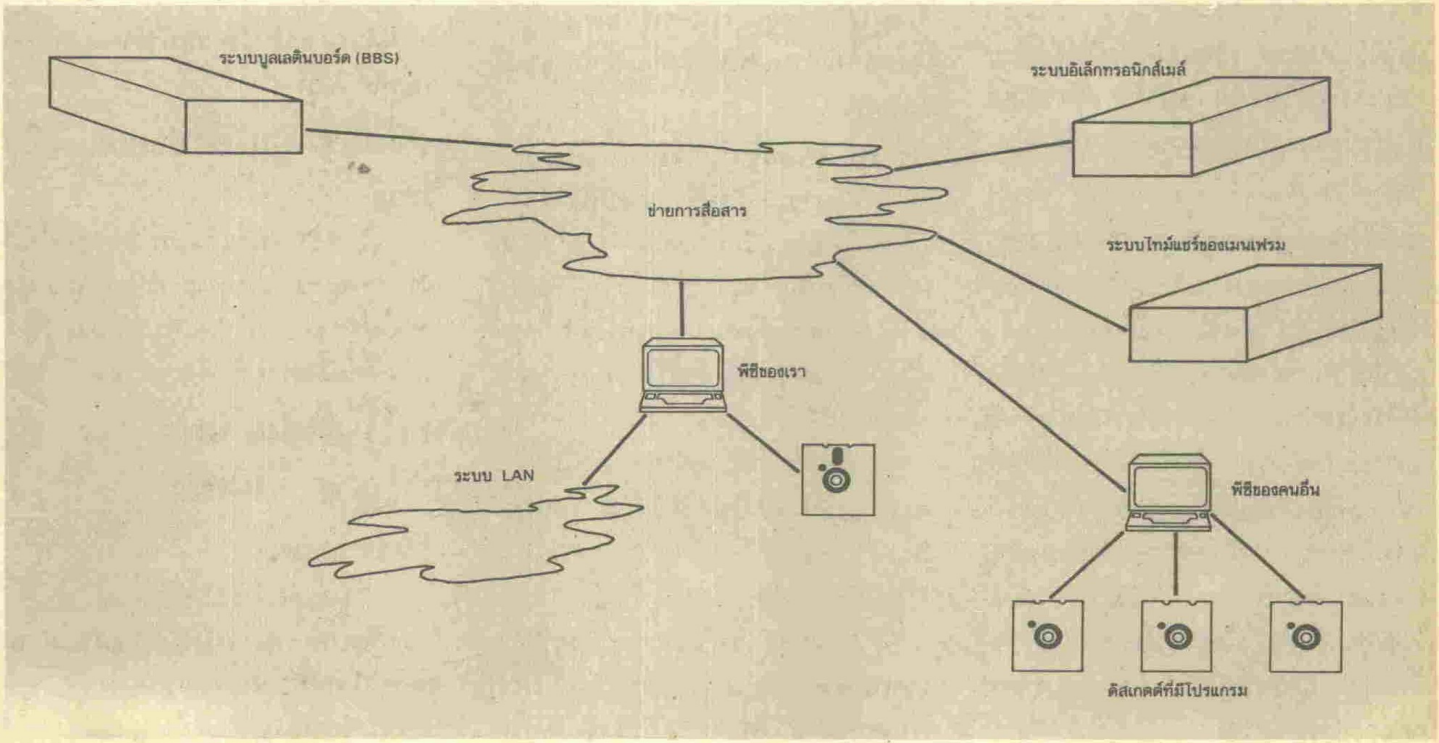
หากพิจารณาดูจากโครงสร้างของไมโครคอมพิวเตอร์เป็นหลักจะพบว่าโอกาสการทำลายของไวรัสที่เป็นไปได้มีหลายจุด เพราะสิ่งเหล่านี้เป็นจุดอ่อนที่ไวรัสจะบุกทำลายได้ จุดอ่อนของไมโครคอมพิวเตอร์ที่อยากขอกล่าวในที่นี้ได้แก่

ไวรัสนำข้อมูลที่เป็นขยะใส่ลงในคอมพิวเตอร์

ไวรัสจะสร้างข้อมูลขึ้นและนำไปเก็บไว้ในที่เก็บต่าง ๆ เช่น ดิสก์ หรือฮาร์ดดิสก์ ทำให้พื้นที่เต็มโดยเร็ว ไวรัสจะทำให้พื้นที่เพิ่มขึ้นโดยการคัดลอกข้อมูลหรือตัวโปรแกรมซ้ำแล้วซ้ำเล่าเข้าเก็บในดิสก์

ขม้ำไฟล์

เนื่องจากระบบไฟล์ของไมโครคอมพิวเตอร์ เป็นสิ่งที่เปิดเผยมากพอ



ควร ดังนั้นจึงเป็นจุดอ่อนให้ไวรัสเข้าไปขม้ำข้อมูลในส่วนต่าง ๆ ในลักษณะชอนไชได้

เขมือบ FAT

FAT หรือ File Allocation Table คือ ส่วนของตารางที่ทำหน้าที่กำหนดการใช้พื้นที่ ดังนั้นหากไวรัสเขมือบ FAT ก็เท่ากับว่าพื้นที่ของดิสค์ที่แท้จริงไม่สามารถอ้างอิงได้ ข้อมูลอยู่ในนั้นก็จะเรียกใช้ไม่ได้อีกต่อไป

จัดการบูตเซกเตอร์

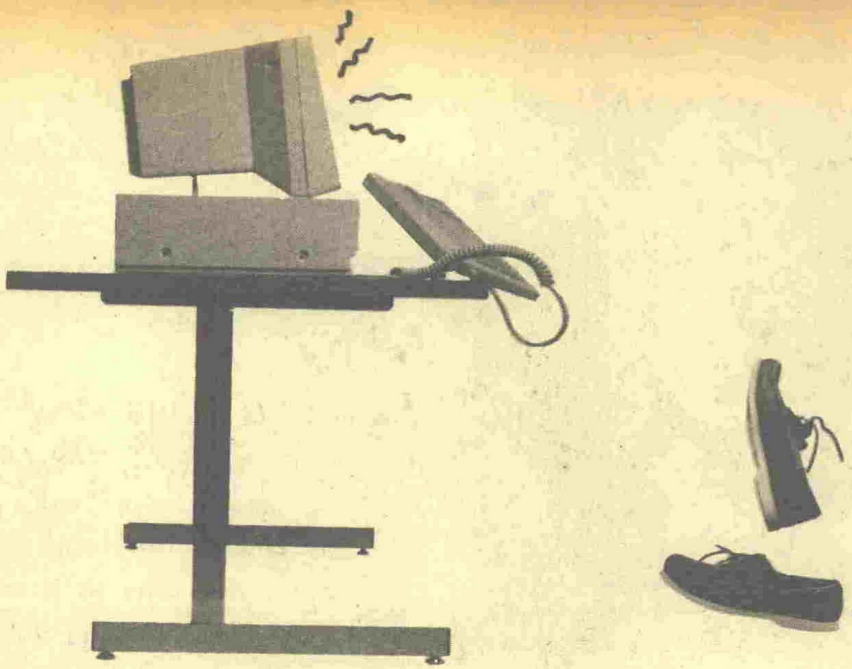
บูตเซกเตอร์เป็นส่วนสำคัญของดิสค์ที่มีข้อมูลสำหรับการบูต ข้อมูลส่วนนี้จำเป็นต่อการเรียกโปรแกรมระบบ ไวรัสจะทำการเปลี่ยนข้อมูลของบูตเซกเตอร์มาเป็นโปรแกรมของตัวไวรัสหรือใส่ข้อมูลที่ไม่พึงประสงค์ เพื่อให้ดิสค์นั้นไม่สามารถเรียกโปรแกรมระบบได้

ฟอร์แมตดิสค์ใหม่เสียเลย

นับว่าเป็นเรื่องที่เลวร้ายมาก ไวรัสจะทำการฟอร์แมตแผ่นใหม่เลย หรือเข้าขั้นทำลายแบบไม่ให้เหลือซากกันเลย ปกติโปรแกรมไวรัสจะค้นหาโปรแกรม FORMAT ในแผ่นดิสค์ ถ้าพบก็จะเรียกมาฟอร์แมต และมักจะฟอร์แมตฮาร์ดดิสค์เสียด้วย

ส่งข้อความมากวนบนจอภาพ

ผู้เขียนโปรแกรมไวรัสมีจิตใจเหมือนคนวิปริต ดังนั้นอาจจะนำข้อความบางอย่างที่เห็นแล้วตกใจมาแสดงบนจอภาพได้ หากท่านพบคำเสาวรสเหล่านั้นก็ขอให้ปลงก็แล้วกัน ในไวรัสบางพันธุ์ที่ใช้กับเครื่องที่แสดงผลแบบกราฟิก เช่น แมคอินทอช มีการทำลายรูปภาพในลักษณะกัดกร่อนทีละเล็กทีละน้อย หรือในพีซี ไวรัสบางพันธุ์ส่งข้อความเป็นขีดรบกวนการแสดงผลบนจอภาพจนดูคล้ายกับว่าฮาร์ดแวร์เสีย



ส่งข้อความออกทางเครื่องพิมพ์

ไวรัสที่จู่โจมในลักษณะนี้ไม่ใคร่พบ แต่ก็เป็นจุดที่ไวรัสจะเข้าโจมตีได้ ไวรัสอาจตรวจสอบว่าระบบต่อกับเครื่องพิมพ์หรือไม่ เครื่องพิมพ์อยู่ในสภาพพร้อมหรือไม่ หากได้โอกาสก็จะส่งข้อความสนุก ๆ ของคนชอบสนุกออกมาทางเครื่องพิมพ์ จุดนี้ก็เป็นจุดที่ทำได้ไม่ยาก

รีเซตคอมพิวเตอร์เสียดื้อ ๆ

เนื่องจากระบบไมโครคอมพิวเตอร์มีวิธีการเรียกเข้าสู่ cold boot หรือรีเซตได้ไม่ยาก ไวรัสจะเรียกโปรแกรมดอสกลับเข้ามาใหม่เสียดื้อ ๆ กลางทางการทำงาน

แขวน (hang) เครื่องเสียเลย

อาการแขวนหรือแฮงนี้ทำได้ง่ายมาก โดยการเรียกคำสั่ง Halt ก็ได้ หรือทำให้เกิดโอเวอร์โฟล์วในซีพียูซะก็ได้ หรือจะให้โปรแกรมลูปไม่ไปไหนก็ได้ จุดอ่อนนี้เป็นจุดที่ก่อกวนระบบและอาจสร้างผลอย่างอื่นตามมา เช่น หากเปิดไฟล์แล้วไม่ปิดแต่เครื่องมีปัญหา ผลก็คือข้อมูลในไฟล์ไม่ได้รับการปรับปรุง

ทำงานช้าลง

ไวรัสหลายพันธุ์แทรกตัวเองลงในหน่วยความจำแล้วย้ายอินเตอร์รัพต์เวกเตอร์มายังโปรแกรมตนเอง ดังนั้นการทำงานหลายขั้นตอนจะต้องผ่านโปรแกรมไวรัสก่อน ผลจะทำให้การทำงานช้าลง

เปลี่ยนค่าแป้นพิมพ์

จุดนี้เป็นจุดที่ไวรัสเข้าไปเปลี่ยนข้อมูลตารางของคีย์บอร์ด ทำให้เมื่อกดคีย์ตัวหนึ่งแต่ได้อักษรอีกตัวหนึ่ง ทำให้ผู้ใช้นึกว่าคีย์บอร์ดมีปัญหา

ล็อกแป้นพิมพ์

หากมีการลบข้อมูลตารางหมดหรือใส่ช่องว่างลงไปแทนตารางแมพของแป้นพิมพ์ ผลคือเมื่อกดคีย์แล้วก็ไม่ได้ตัวอักษรอะไรออกมาจึงเหมือนการล็อกคีย์บอร์ด

เปลี่ยนข้อมูลในโปรแกรมหรือไฟล์

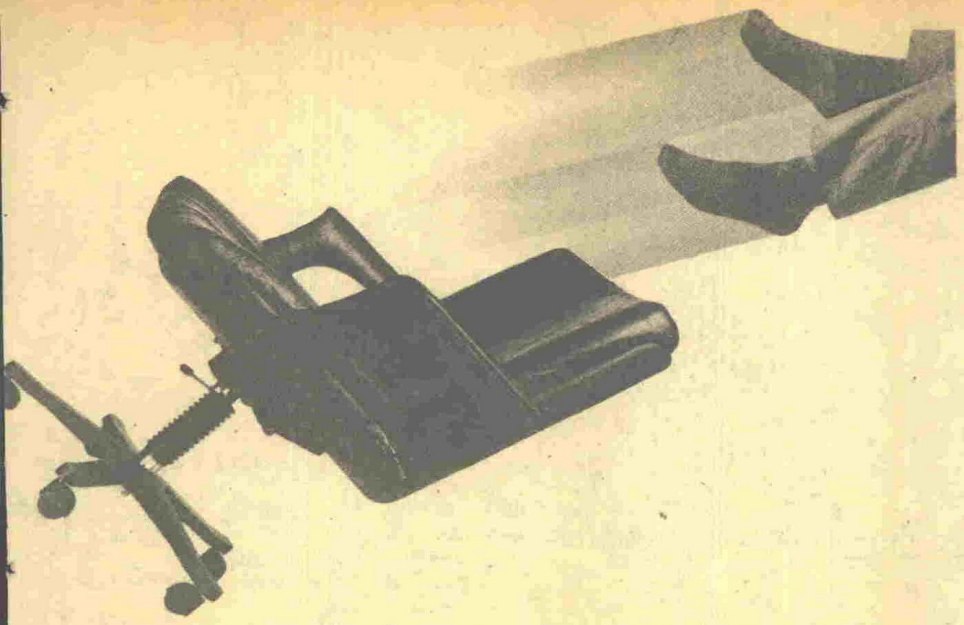
ไวรัสบางพันธุ์จะทำการเปลี่ยนแปลงข้อมูลบางส่วนของโปรแกรม ทำให้เมื่อทำงานในโปรแกรมนั้นจะรู้สึกเหมือนโปรแกรมมีข้อบกพร่อง

ทำให้ฮาร์ดดิสค์มีปัญหาต้องทำ

ปรีฟอร์แมต

ส่วนของฮาร์ดดิสค์มีจุดอ่อนมาก หากเราสามารถทำให้ฮาร์ดดิสค์ในส่วนของข้อมูลบางเซกเตอร์มีปัญหา เช่น ในส่วนที่กำหนดพาร์ติชัน

เทคนิคไวรัส



คัดลอกโปรแกรมไปไว้ในไดเรคทอรีอื่นที่อยู่ในไดรฟ์

ไวรัสอาจตีรวนคัดลอกข้อมูลจากไดเรคทอรีหนึ่งไปไว้ในอีกไดเรคทอรีเพื่อเพิ่มขนาดการใช้ดิสค์หรือทำให้ผู้ใช้ปวดหัวเล่น ว่าอยู่ ๆ มีข้อมูลเกิดขึ้นในไดเรคทอรีของตนได้อย่างไร

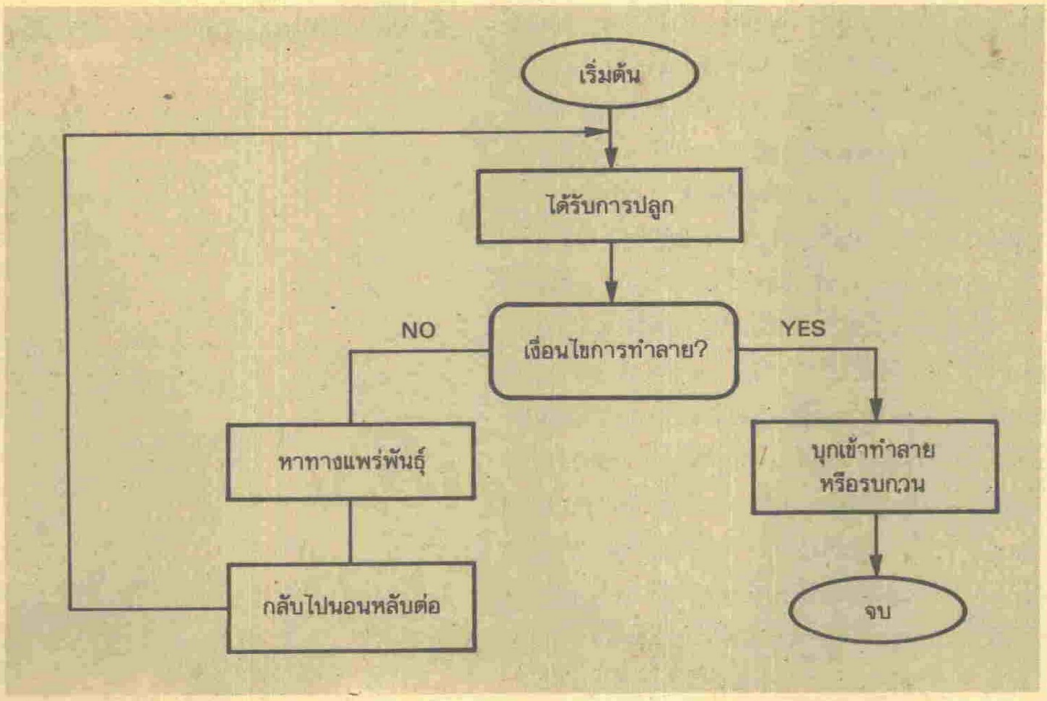
วิเคราะห์คุณสมบัติของไวรัส

จากที่กล่าวในที่นี้แล้วว่า ไวรัสคือโปรแกรมคอมพิวเตอร์ที่สามารถแพร่ขยายจำนวนและทำลายสร้างความเสียหายจนเป็นที่กล่าวขวัญกันทั่วเมืองได้ โปรแกรมไวรัสจึงเป็นโปรแกรมคอมพิวเตอร์ซึ่งจะต้องมีคุณลักษณะพิเศษ คือ ซ่อนตัวเองโดยไม่ให้ผู้ใดรู้ และจะได้รับการปลุกหรือถูกเรียกให้รันได้ และเมื่อมันทำงานมันก็จะหาทางขยายแบ่งพันธุ์ตัวเองโดยไม่ให้ใครรู้ หรืออาจจะทำลายตามจุดอ่อนของระบบดังที่กล่าวมาแล้ว โครงสร้างคุณสมบัติของไวรัสจึงเขียนแสดงได้ดังรูปที่ 4

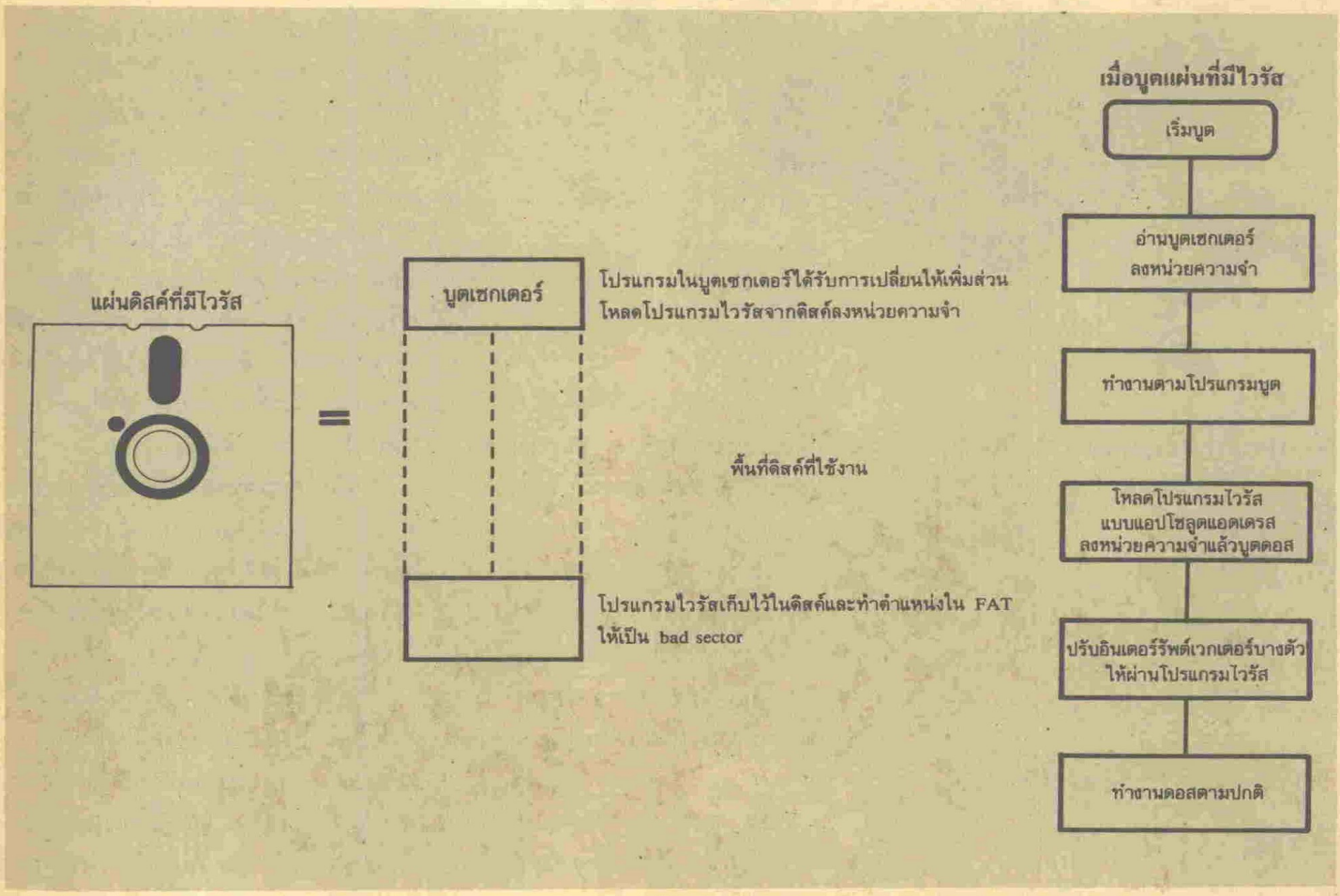
จากคุณสมบัติดังรูปที่ 4 เป็นคุณสมบัติพื้นฐานของไวรัส ในที่นี้จะขอขยายความเพื่อให้เห็นภาพการทำงานชัดเจนขึ้น (ผู้อ่านอาจหาอ่านโครงสร้างของไบออสหรือดอสเพิ่มเติมจากหนังสือไมโครคอมพิวเตอร์ 16 บิต ที่บริษัทซีเอ็ดยูเคชั่น จัดพิมพ์เพื่อประกอบหลักการก็จะเข้าใจยิ่งขึ้น) โครงสร้างสมบัติของไวรัสตัวนี้ คือตัวที่พบในเมืองไทยตัวแรก ๆ ที่ผู้เขียนจะเน้นให้เห็น ประกอบเป็นไดอะแกรมดังรูปที่ 5

เมื่อเรียกอินเตอร์รัพต์เวกเตอร์ที่ผ่านไวรัส จะเป็นการปลุกไวรัสให้ตื่นเพื่อทำงานบางสิ่งบางอย่างตามที่เขียนไว้ในตัวไวรัส ไดอะแกรมการทำงานจะเป็นดังรูปที่ 6

หากพิจารณาจากทำงานนี้แล้ว ผู้ที่เข้าใจโครงสร้างของไมโครคอมพิวเตอร์ 16 บิต จะเขียนโปรแกรมนี้ได้ไม่ยาก แต่โครงสร้างไวรัสนี้ยังพื้น ๆ และอัตราการแพร่ขยายไม่มาก เพราะจะแพร่ได้ต้องนำดิสค์ที่มีไวรัสมาบูต ตัว



รูปที่ 4
โครงสร้างคุณสมบัติของไวรัส



รูปที่ 6
แสดงการเริ่มบูตไวรัสเข้าหน่วยความจำ

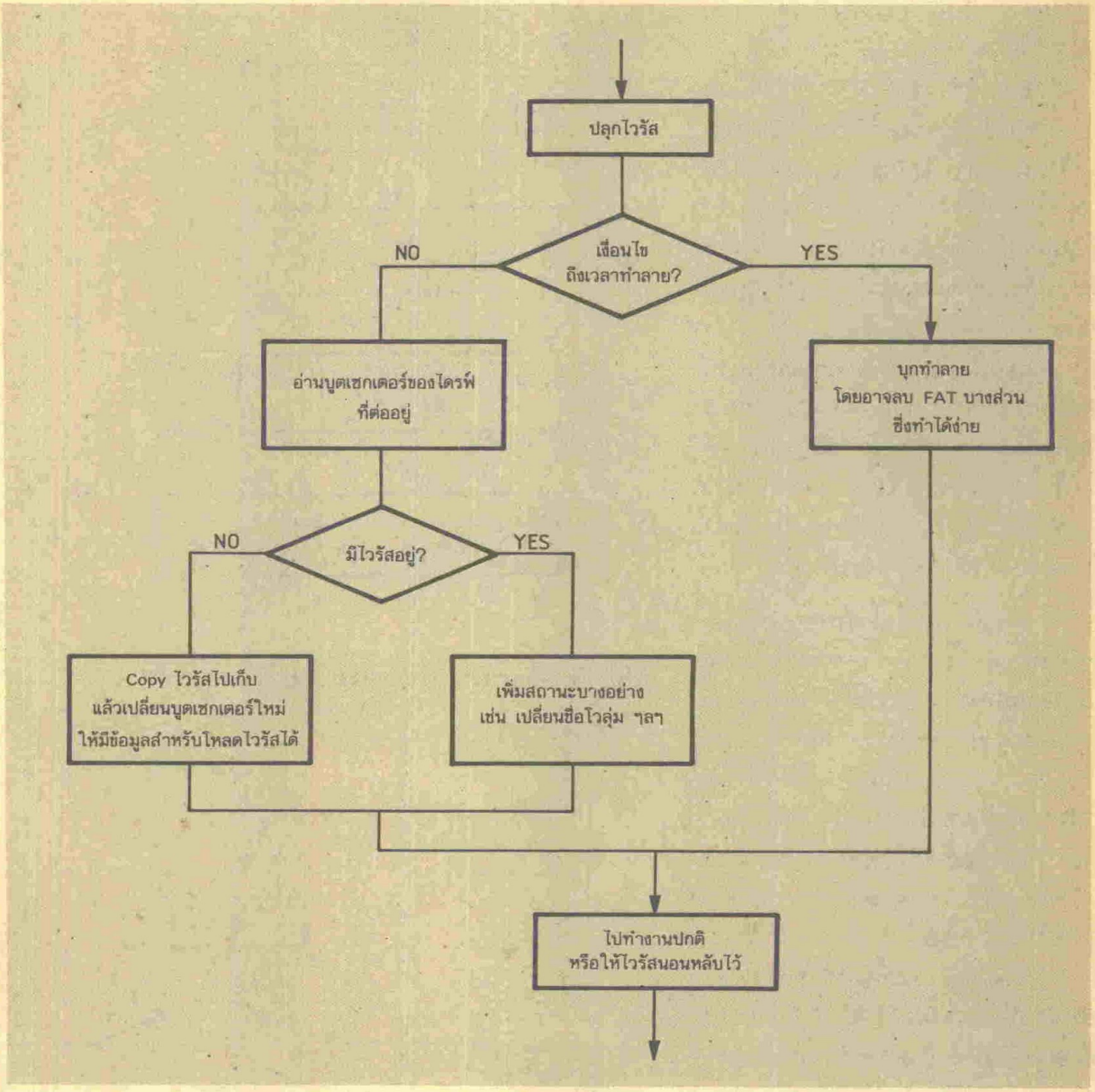
ไวรัสจึงจะอยู่ในหน่วยความจำแล้วแพร่ขยายไปยังดิสค์แผ่นอื่นได้ การแพร่ขยายวิธีนี้เป็นไวรัสที่พบในเมืองไทยยุคแรก การกำจัดจึงเพียงแต่ดูที่บูตเซกเตอร์เท่านั้นก็จะพบว่ามีไวรัสอยู่บนดิสค์หรือไม่

ลักษณะไวรัสที่แพร่ขยายได้เร็วต้องเกาะกับไฟล์

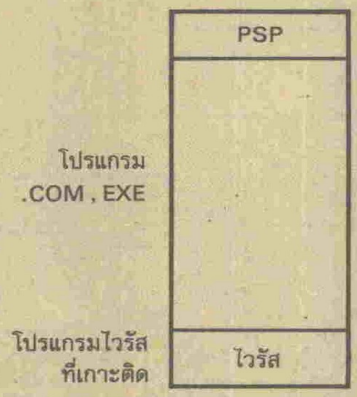
การใช้งานไมโครคอมพิวเตอร์ส่วนใหญ่จะมีการโหลดเรียกไฟล์ .EXE หรือ .COM หรือเรียกไฟล์ข้อมูลมาใช้อยู่เสมอ ดังนั้นถ้าให้ไวรัสเกาะกับไฟล์เหล่านี้ โอกาสของไวรัสจะเข้าไปนอนในหน่วยความจำก็มีสูงมากขึ้น เมื่อปลุกไวรัส ไวรัสก็แพร่เกาะเข้าในไฟล์อื่น ๆ ได้โดยง่าย อัตราการติดต่อจึงสูงมาก การแพร่กระจายจะรวดเร็วและแพร่ได้ทุกทาง ทั้งทางการสื่อสารข้อมูล การแลกเปลี่ยนระหว่างเครื่องด้วยวิธีอื่นใดก็ตามก็แพร่กระจายไปได้ โครงสร้างของไวรัสประเภทนี้เขียนเป็นไดอะแกรมได้ ดังรูปที่ 7

โปรแกรมที่ติดไวรัสนี้จะเป็นสื่อพาหะในการนำเอาไวรัสลงสู่หน่วยความจำ ดังนั้นเมื่อมีการเรียกโปรแกรมที่มีไวรัสนี้มาทำงาน โครงสร้างการถ่าย CS:IP หรือจุดเริ่มของการทำงานจะมายังตัวไวรัสก่อน ตัวโปรแกรมไวรัสจะไปเปลี่ยนแปลงอินเตอร์รัพต์เวกเตอร์เพื่อไว้ใช้ในการปลุกไวรัส หลังจากนั้นก็จะกระโดดไปทำงานโปรแกรมที่โหลดลงมานั้นอย่างปกติ ผู้ใช้งานก็จะไม่รู้ว่ามีอะไรเกิดขึ้น โครงสร้างการโหลดโปร-

รูปที่ 6
ผังงานของ
โปรแกรมไวรัส



รูปที่ 7
โครงสร้างของไวรัส
ที่เกาะติดไฟล์ .COM, .EXE



โปรแกรม .COM หรือ .EXE จะถูกดัดแปลงมาก่อน โดยให้จุด entry ของโปรแกรมมายังโปรแกรมไวรัส ในตอนเริ่มต้นได้ ดังนั้น .COM จึงมักพบไวรัสอยู่ตอนบน .EXE จะมีไวรัสอยู่ตอนล่าง

แกรมที่มีไวรัสลงมาแสดงเป็นลำดับขั้นดังรูปที่ 8

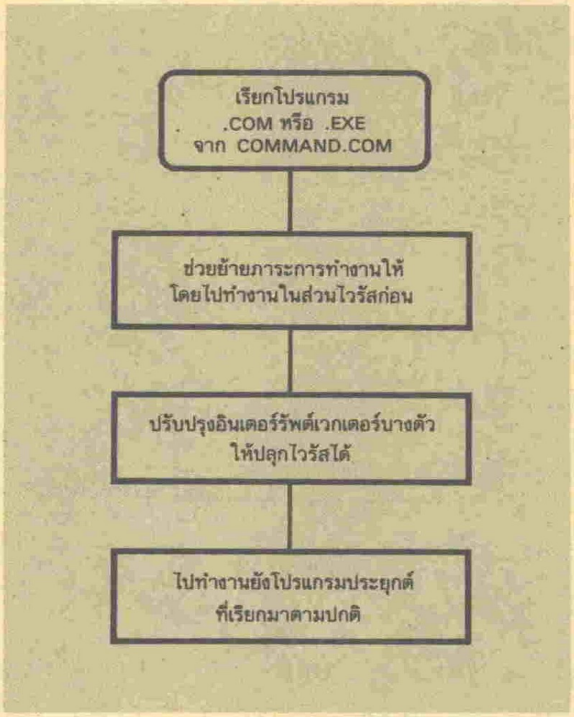
สังเกตว่าวิธีการนำเอาโปรแกรมไวรัสลงหน่วยความจำนี้ทำได้ง่ายมาก เพราะโปรแกรมไวรัสเป็นส่วนหนึ่งที่ติดอยู่กับโปรแกรมที่เรียกเข้ามาอยู่แล้ว ไวรัสจึงมีโอกาสนอนรออยู่ในหน่วยความจำ รอการปลุกมาแพร่พันธุ์ หรือทำลายในเวลาต่อมาได้

ครั้นถึงเมื่อมีการทำงานเรียกผ่านอินเตอร์รัพต์เวกเตอร์ ตัวที่เปลี่ยนค่าให้วิ่งมาหาตัวไวรัส ไวรัสก็ถูกปลุกให้ตื่นขึ้นมา และจะมีการทำงานตามโปรแกรมไวรัสทันที ผังงานของโปรแกรมไวรัสในกรณีนี้ เป็นดังรูปที่ 9

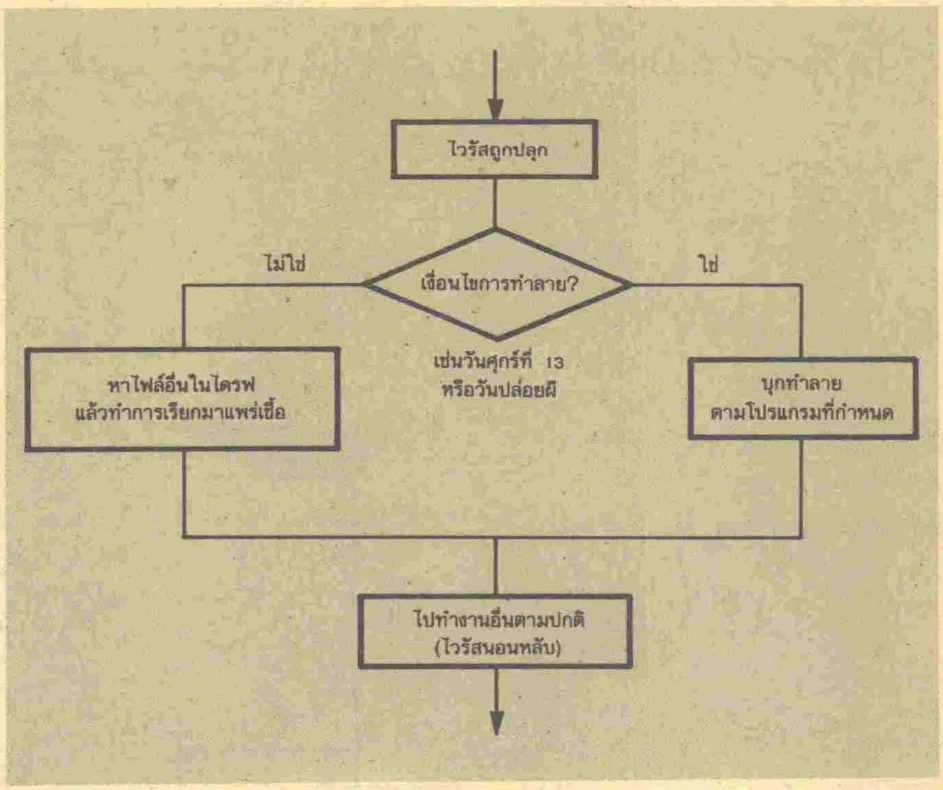
การทำงานของไวรัสที่กล่าวนี้เป็นขั้นตอนอย่างหยาบ ๆ การแพร่กระจายมีเทคนิคค้นหาตัวพาหะได้หลายอย่าง โดยเฉพาะเมื่อใช้กับฮาร์ดดิสก์ที่มีไดเรคทอรีย่อยหลายตัว โปรแกรมจะต้องทำงานโดยย้ายไปค้นหาในไดเรคทอรีย่อยอื่น ๆ ได้ โปรแกรมไวรัสจึงเขียนให้ยุ่งยากหรือเพิ่มประสิทธิภาพการขยายตัวได้อีกมาดังรูปที่ 10

ผังของไวรัสที่มีอัตราการแพร่พันธุ์สูงนี้ เริ่มจากการปลุกไวรัส ไวรัสจะเซตค่าเริ่มต้นโดยการตรวจสอบดูว่าตอนนี้กำลังติดต่อกับไดร์ฟใดอยู่ ตรวจสอบดูเงื่อนไขว่าพร้อมให้ทำลายแล้วหรือยัง เช่น ตรงกับวันปล่อยผีแล้วหรือยัง (บางคนเขียนไวรัสขึ้นเพื่อความโกรธแค้น พอถึงวันชาติของอีกประเทศหนึ่งที่เป็นคู่แค้นสั่งไวรัสจู่โจม) ในการทำลายก็ทำลายแบบรุนแรง ก็คือ การฟอร์แมตดิสก์ใหม่ โดยเน้นพยายามจะฟอร์แมตฮาร์ดดิสก์ก่อน ถ้าไม่มีก็ฟอร์แมตฟลอปปี้ดิสก์

หากยังไม่ถึงโอกาสทำลาย ก็เริ่มหาดูว่ามีไดรฟ์อื่นต่ออยู่หรือไม่ ถ้ามีก็

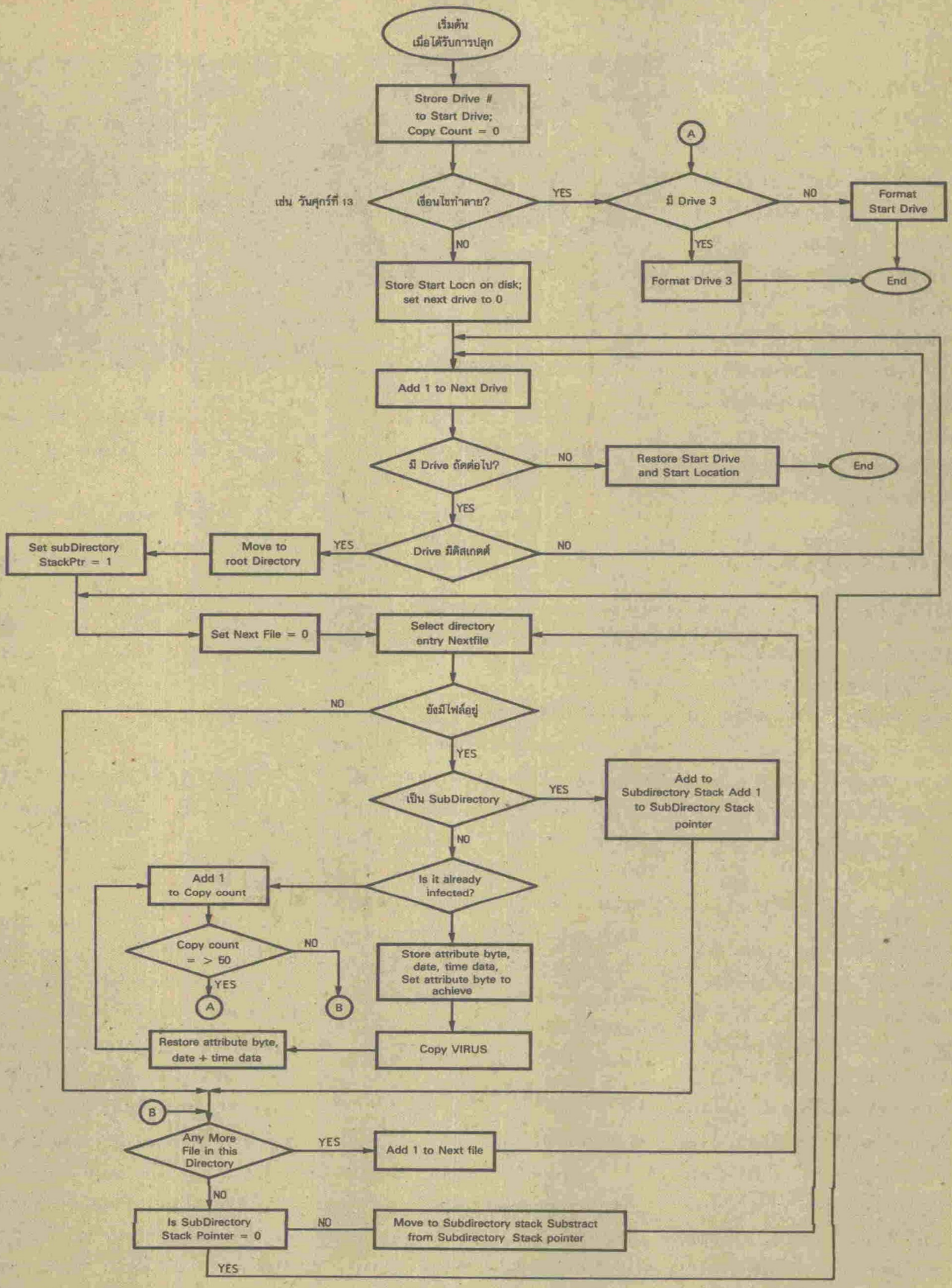


รูปที่ 8 ลำดับการเรียกโปรแกรม .COM, EXE ที่มีไวรัส



รูปที่ 9 ผังการทำงานของไวรัสเมื่อถูกปลุก

รูปที่ 10 ผิวของไวรัสที่มีอัตราการแพร่พันธุ์สูง →


เริ่มต้น
เมื่อได้รับการปลุก
Strore Drive #
to Start Drive;
Copy Count = 0
เช่น วันศุกร์ที่ 13
เชื้อนไขทำลาย?
YES
มี Drive 3
NO
Format
Start Drive
NO
YES
Store Start Locn on disk;
set next drive to 0
Format Drive 3
End
A
Add 1 to Next Drive
มี Drive ถัดต่อไป?
NO
Restore Start Drive
and Start Location
End
YES
Set subDirectory
StackPtr = 1
Move to
root Directory
YES
Drive มีดิสเกตต์
NO
Set Next File = 0
Select directory
entry Nextfile
NO
ยังมีไฟล์อยู่
YES
เป็น SubDirectory
YES
Add to
Subdirectory Stack Add 1
to SubDirectory Stack
pointer
NO
Add 1
to Copy count
Is it already
infected?
Copy count
= > 50
NO
YES
A
B
Store attribute byte,
date, time data,
Set attribute byte to
achieve
Restore attribute byte,
date + time data
Copy VIRUS
B
Any More
File in this
Directory
YES
Add 1 to Next file
NO
Is SubDirectory
Stack Pointer = 0
NO
Move to Subdirectory stack Substract
from Subdirectory Stack pointer
YES

ไปดูทีละไดเรคทอรี แล้วเข้าไปทีละไฟล์ เพื่อแพร่ขยายพันธุ์ เมื่อครบทุกไฟล์ในไดเรคทอรีแล้วก็ย้ายไปทำทีละไดเรคทอรีจนหมด ดังนั้นทุกไฟล์ในดิสค์จะติดไวรัสหมด ไฟล์เหล่านี้ถ้าให้ใครไปหรือได้รับการเรียกลงใหม่ มันก็จะเตรียมพร้อมขยายอีกไม่มีที่สิ้นสุด ไวรัสจึงขยายพันธุ์ได้รวดเร็วมาก และเกาะไปกับโปรแกรมโดยที่ผู้ใช้ทั่วไปไม่มีโอกาสรู้

ไวรัสบางตัวใช้วิธีการพอกไวรัสเข้ากับโปรแกรมอื่นไปเรื่อย ๆ ทำให้ขนาดของโปรแกรมนั้นโตขึ้นทีละน้อย ในที่สุดดิสค์ที่ใช้ก็เต็ม หรือโปรแกรมใหญ่พอโหลดลงหน่วยความจำไม่ได้

เราจะสร้างวัคซีนได้อย่างไร

หากรู้ลักษณะของไวรัสที่แน่ชัดแล้วเราก็มีวิธีที่จะต่อสู้กับไวรัสได้ การต่อสู้กับไวรัสจึงมีรูปแบบการต่อสู้ 3 รูปแบบ คือ

1. การตรวจหาไวรัส
2. การป้องกันไวรัส
3. การทำลายไวรัสหรือซ่อมแซมส่วนที่ไวรัสทำลาย

การตรวจหาไวรัส

เป็นวิธีหนึ่งที่เราสามารถตรวจหาได้ไม่ยาก เช่น ไวรัสที่เปลี่ยนข้อมูลในบูตเซกเตอร์(ไวรัสตัวแรก ๆ ที่เข้าเมืองไทย) เราก็เขียนโปรแกรมตรวจหาข้อมูลที่เปลี่ยนไปในบูตเซกเตอร์ โดยปกติเราสามารถบอกได้โดยดูจากบูตเซกเตอร์แผ่นที่ไม่ติดไวรัสกับแผ่นที่มีไวรัสมาเปรียบเทียบหาส่วนต่าง การเขียนโปรแกรมดูส่วนนี้ก็เป็นวิธีที่ทำให้เราทราบว่ามีไวรัสแล้วในแผ่นนี้ เพื่อจะได้ทำลายหรือฟอร์แมตแผ่นใหม่ สำหรับไวรัสบางตัวที่เกาะอยู่กับไฟล์ เช่น เกาะที่ไฟล์ Command.com ก็ตรวจหาส่วนต่างหรือ string pattern บางอย่างที่มีในไฟล์ การตรวจหาในกรณีง่าย ๆ อีกวิธีหนึ่ง คือ ดูขนาดของไฟล์ที่เปลี่ยนไป(ถ้าเรามีข้อมูลขนาดของไฟล์เดิมอยู่) การตรวจหาไวรัสจึงเป็นวิธีที่ผู้ใช้ใช้ในการสแกนหาได้ ไวรัสแต่ละตัวจะมีลักษณะแตกต่างกันไป เราจึงต้องศึกษาไวรัสพันธุ์ต่าง ๆ ไว้

การป้องกันไวรัส

เป็นเทคนิคที่มีผู้พยายามทำกันเพื่อเอาชนะไวรัส เช่น ตรวจสอบโพลีโนเมียล หรือขนาดของไฟล์ หรือ CRC ของไฟล์ในโปรแกรม หากข้อมูลในไฟล์มีการเปลี่ยนแปลงไปก็จะบอก หรือกรณีของไฟล์ที่ใช้งาน เช่น .COM หรือ .EXE จะทำให้กลไกไม่สามารถเขียนลงมาได้เลย การป้องกันไวรัสเป็นเรื่องที่ทำได้ยากกว่าการตรวจหา ดังนั้นโปรแกรมที่ตั้งชื่อว่าวัคซีน ส่วนใหญ่มิได้ป้องกันแต่เป็นการตรวจหาและแก้ไข

การทำลายไวรัสและซ่อมแซมส่วนที่ไวรัสทำลาย

ส่วนนี้ก็ต้องรู้ลักษณะของโปรแกรมไวรัสและวิธีการทำลายของไวรัสเป็นอย่างดี โปรแกรมแก้ไขและทำลายไวรัสในบางตัวทำได้ง่าย เช่น โปรแกรมแก้ไขไวรัสในส่วนที่เกาะมากับดิสค์และแก้บูตเซกเตอร์ ถ้าเราแก้ไขบูตเซกเตอร์กลับไปตัวเดิม ไวรัสก็จะถูกทำลายไปนั่นเอง

"ไม่มีวัคซีนขนานใดในโลกจะป้องกันไวรัสได้ทุกชนิด"

ดังนั้นวัคซีนแต่ละตัวจะใช้จัดการกับไวรัสเป็นตัว ๆ ไป และเราจะพบไวรัสพันธุ์ใหม่เกิดขึ้นเรื่อย ๆ และก็จะมีวัคซีนตัวใหม่เกิดขึ้นเรื่อย ๆ วนเวียนกันเป็นวัฏจักร

ไวรัสคอมพิวเตอร์แบบ "เอดส์" จะเกิดขึ้นได้หรือไม่

ว่ากันว่า "เอดส์" เป็นไวรัสที่ถูกส่งมาท้าทายความสามารถมนุษย์ ไวรัสของเอดส์มีคุณสมบัติแปรเปลี่ยนตลอดเวลา จนทำให้นักวิทยาศาสตร์ไม่สามารถศึกษาหาโครงสร้างของมันได้ หากไวรัสคอมพิวเตอร์มีการปรับเปลี่ยนตัวโปรแกรมของมันได้เองโดยมันจะผันแปรไปได้ตลอดเวลา เมื่อนั้นไวรัสคอมพิวเตอร์ตัวนี้ก็จะเป็นตัวที่ยากต่อการพิชิต ไวรัสคอมพิวเตอร์ในปัจจุบันยังเป็นไวรัสที่หาโครงสร้างได้ง่าย ดังนั้นเราจึงหาทางกำจัดมันได้ไม่ยาก และถ้าเราเผยแพร่โครงสร้างเหล่านี้ไปให้ผู้

ใช้ได้มากเท่าไร ผู้ใช้คอมพิวเตอร์ก็จะมีข้อมูลและช่วยกันกำจัดมันได้มากขึ้น และในไม่ช้าไวรัสตัวนั้นก็จะสูญพันธุ์ แต่ถ้าไวรัสคอมพิวเตอร์เป็นแบบ "เอดส์" เราอาจต้องมีการตั้งสถาบันวิจัยไวรัสคอมพิวเตอร์ เพื่อต่อสู้กับมันก็ได้ เมื่อถึงเวลานั้นอะไรจะเกิดขึ้นก็ยากที่จะคาดเดา แต่อยากให้ข้อคิดว่า ถ้าไวรัสติดในคอมพิวเตอร์แล้วกำจัดมันไม่ได้จะเป็นอย่างไร

หนทางปฏิบัติที่อยากฝากไว้

เพื่อให้การใช้คอมพิวเตอร์ของพวกเราเป็นไปอย่างมีความสุข ผู้เขียนขอแนะนำสิ่งเล็ก ๆ น้อย ๆ ที่น่าปฏิบัติดังนี้

- หาโปรแกรมมาใช้จากแหล่งที่เชื่อถือได้ว่าปราศจากไวรัส โปรแกรมที่พัฒนาขึ้นโดยผู้เชี่ยวชาญย่อมให้ความมั่นใจ ดังนั้นการซื้อโปรแกรมจากแหล่งต้นฉบับดูจะมั่นใจได้

- ทุกครั้งที่ได้โปรแกรมใหม่ ให้ทำการติดสติกเกอร์ป้องกันการเขียนลงในแผ่นต้นฉบับทันที

- ให้ทำการก๊อบปี้ตัวโปรแกรมต้นฉบับนั้นไว้เป็นสำรอง และเก็บเอาไว้ การก๊อบปี้ต้องทำในสิ่งที่เชื่อถือได้ เช่น ก๊อบปี้แบบเซกเตอร์ต่อเซกเตอร์ และเก็บแผ่นสำเนานี้ไว้ เมื่อเวลาจะใช้สำหรับการโหลด (Copy) ลงฮาร์ดดิสก์ ให้ใช้แผ่นต้นฉบับจริง

- การติดตั้งโปรแกรม (install) ทุกครั้งต้องทำกับแผ่นที่มีการป้องกันการเขียน

- ให้เก็บข้อมูลของโปรแกรมไว้โดยเฉพาะข้อมูลที่เกี่ยวกับขนาด เพื่อไว้ใช้ในการเปรียบเทียบในภายหลัง

- ให้เก็บแผ่นต้นฉบับดอส และติดป้องกันการเขียนไว้อย่างดี แผ่นนี้จะมีโปรแกรม DISKCOMP ซึ่งสามารถนำมาใช้ตรวจหาไวรัสได้โดยเปรียบเทียบกับโปรแกรมต้นฉบับที่มีการป้องกันการเขียนไว้แล้ว

- หากพบไวรัสเข้ามาให้ลบโปรแกรมหรือฟอร์แมตแผ่นที่มีไวรัสทิ้งทันที การเก็บข้อมูลหรือโปรแกรมที่อยู่ร่วมกับโปรแกรมที่ติดไวรัสนั้นต้องตรวจหาโดยบูตจากแผ่นที่ไม่มีไวรัสแล้วหาดูว่าไวรัสมีที่ใดบ้าง

- ศึกษาลักษณะของไวรัส ถ้ารู้ว่าไวรัสตัวใดมีโครงร่างสตริงข้อความใดอยู่ ค้นหาข้อความนั้นในโปรแกรมที่สงสัย ถ้าพบให้ทำลายทันที วิธีการค้นอาจใช้โปรแกรมจำพวก Norton Commander ช่วยได้

- ให้หมั่นสังเกต BAT ไฟล์ โดยเฉพาะ Autoexec.bat หรือ CONFIG .SYS ว่ามีการเปลี่ยนแปลงข้อมูลเองหรือไม่ เพราะไวรัสบางตัวอาศัยวิธีการโหลดตัวเองผ่านลงไปด้วย AUTOEXEC

- หลีกเลี่ยงความเสี่ยงโดยไม่ให้ผู้อื่นใช้เครื่องโดยนำโปรแกรมของเขามาใช้ เพราะอาจจะทำให้เกิดการแพร่ไวรัสลงฮาร์ดดิสก์ได้

- ในกรณีเครื่องที่มีเฉพาะฟลอปปี้-ดิสก์ทุกครั้งที่มาใช้ต่อจากผู้อื่นให้รีเซตเครื่องเพื่อบูตใหม่ โดยการบูตจากแผ่นดอสที่มีการติดป้องกันการเขียนเอาไว้

- ควรสำเนาข้อมูลสม่ำเสมอ

หากปฏิบัติดังเช่นว่านี้แล้ว ก็คิดว่าท่านคงเป็นผู้หนึ่งที่โชคดีจากไวรัสได้ และหากปฏิบัติดังนี้แล้วยังมีไวรัสมาอาละวาดได้อีก ก็ขอให้นึกเสียว่า เป็นเคราะห์กรรมก็แล้วกันครับ

หวังว่าพวกเราชาวไทยคงไม่มีใครคิดอยากจะสร้างไวรัสนะครับ และอย่ามีจดหมายมากวนผมนะครับว่า ช่วยสร้างไวรัสให้หน่อย หรือส่งโปรแกรมไวรัสเป็นของฝาก ผมไม่เล่นด้วยแน่ ๆ